Segurança da Informação nas Redes Sociais

David Carvalho Dos Reis [1], ***Claudineia Helena Recco***[1], **Marcelo Eloy Fernandes**[1]

[1]Departamento de Pós-Graduação– *Universidade Nove de Julho, UNINOVE*

01156-050, São Paulo - SP – Brazil

davidreis631@hotmail.com, {chrecco,marceloeloyfernandes}@gmail.com

Abstract. The period leading social networks be it simple communication through a home phone, or even in the times of war, have evolved until it reaches the form of communication we see today. Social networks with the help of the internet is the easiest guy to socialize today, because there is no need for travel. It is possible to say that, over the years, it has become increasingly commonplace to see. Certainly, there are numerous possibilities for access, either through laptops, tablets or smatphones, among others, however, the objective will point better understanding of the various forms of vulnerability that may occur in the use of social networks, and how it could have a considerable impact on human reality. For this, we will present "tools" demonstration, which may explain the main cases of invasion and how to use the form of networks that is safer for the sender and the receiver.

Resumo. O período que antecede as redes sociais seja comunicação simples através de um telefone residencial, ou até mesmo nos tempos da guerra, foram evoluindo até chegar à forma de comunicação que vemos hoje. As redes sociais com o auxílio da internet são a forma mais fácil do indivíduo se socializar nos dias atuais, pois não há a necessidade de locomoção. Decerto, existem inúmeras possibilidades de acesso, seja através de notebooks, tablets ou smatphones, entre outros, contudo, o objetivo será apontar um melhor entendimento sobre as diversas formas de vulnerabilidade que podem ocorrer no uso das redes sociais, e como isso poderá causar um impacto considerável na realidade humana. Para isso, apresentaremos "ferramentas" demonstrativas, as quais podem explicitar os principais casos de invasão e como devemos utilizar as redes de forma que seja mais seguro para o emissor e para o receptor.

1. Introdução

Esse artigo tem como objetivo entender, alertar e apontar diversas formas de ataques seja por engenharia social, *spam*, *trojan* ou vírus, recorrentes em diversas situações e aplicações, demonstrando que o uso das redes sociais, quando tomadas as devidas precauções é uma ótima ferramenta de comunicação.

Cada vez mais é possível percebermos que, as redes sociais são uma forma de comunicação em duas vias. São utilizadas tanto para se comunicar entre indivíduos, compartilhar experiências, além de possibilitar a interação com pessoas de qualquer região do mundo, nessa pesquisa irá abordar as mais usuais, dentre as quais *Facebook*, *Twitter, WhatsApp, Instaram, Google+, LinkedIn* e outras. Existem algumas diferenças e formas de abordagem que iremos relatar mais à frente.

Devido à grande quantidade de usuários dessas redes sociais e a quantidade de informações trafegadas e armazenadas em seus servidores, estas são diariamente testadas por ataques cibernéticos recebidos por todo mundo, avaliando sua vulnerabilidade e testando a ingenuidade de seus usuários. Porém às vezes a maior parte das ameaças parte do próprio usuário, que indevidamente acabam fornecendo dados e facilitando o trabalho de grupos de *hackers*.

De acordo com pesquisas na literatura e realizada vai Google forms , as redes sociais criadas virtualmente são fundamentais para a troca de informações, contato e encontro de pessoas, mas afetam os relacionamentos de uma forma bem geral, e podem ser usadas tanto para o "bem" quanto para o "mal". Este mundo virtual social é integrado por diversos tipos de pessoas. Visto que não existe filtro real de idade, caráter ou de personalidade, qualquer pessoa pode ter acesso às redes sociais hoje em dia. E é através desta permissividade que crianças conseguem trocar informações com usuários, sem ao menos saber com quem está se relacionando do outro lado da rede, que pode ser um criminoso (WENDT, 2010).

2. Segurança da Informação e Seus Princípios

A segurança da informação diz respeito à proteção de determinado dado ou informação, com a intenção de preservar seus respectivos valores para uma organização, seja empresa ou pessoa física. Podemos então entender como informação todo conteúdo ou dado valioso, isso consiste em qualquer conteúdo com capacidade de armazenamento ou transferência e que seja de utilidade do ser humano.

Com passar dos tempos essa informação foi sofrendo mudanças e hoje é em quase sua totalidade digital, necessitando desta forma, ser propositalmente

confidencializada. A segurança de determinadas informações pode ser afetada por vários fatores, como: os comportamentais e principalmente do usuário, seja pelo ambiente ou pelo fator da infraestrutura em que será trafegada (BENETTI, 2015).

Portanto existem três pilares de segurança que devem ser seguidos, para que se tenha um ambiente mais seguro e consequente uma tranquilidade maior na utilização dos meios digitais, que são (BENETTI, 2015:

Confidencialidade: É garantir que apenas pessoas autorizadas tenham acesso à informação, mantendo os dados confidenciais apenas aos de direito ao acesso.

Integridade: Garantir que os dados não sejam alterados e ou modificados por pessoas que não possuam autorização.

Disponibilidade: Manter a informação disponível sempre que a mesma for requisitada por quem de direito.

3. Redes Sociais

Antes de abordar o início das redes sociais no Brasil, vamos fazer um apanhado da história das redes sociais ao redor do mundo.

Nos últimos 10 anos houve um grande avanço na questão do uso das redes sociais, uma grande revolução na forma de comunicação, pesquisas na literatura relatam que serviços com características das redes sociais das quais conhecemos hoje, iniciaram por volta de 1969 nos EUA que na época utilizava o *dial-up* como forma de conexão. Até chegar mais tarde, exatamente em 1971 quando houve a criação do *Bulletin Board system* (BBS), que foi um sistema criado para convidar amigos para eventos e realizar anúncios pessoais (SANTANA, 2006).

Em 1994 foi apresentado pela primeira vez no mundo, o *GeoCities*, com o conceito de oferecer recursos para que as pessoas criassem suas próprias páginas na web de acordo com sua geolocalização, seu serviço ficou operante até meados de 2009, quando foi encerrado definitivamente (SANTANA, 2006).

Porém as redes sociais como vemos nos dias de hoje, só surgiram por volta dos anos 2000, onde as principais foram *Flickr*, para os amantes de fotografias, o *Orkut* e o *Facebook*. A seguir apresentaremos as características apresentadas pelas principais redes sociais da atualidade.

Facebook: Criada em fevereiro de 2004 por Mark Zuckerberg, Dustin Moskovitz e Chris Hughes, então alunos da Universidade de *Harvad*, onde desde sua criação teve sempre como objetivo principal, a configuração de um espaço onde pessoas pudessem encontrar outras e compartilhar experiências, ficando limitada apenas ao campus da universidade. E a partir de 2006 foi permitido que trabalhadores de empresas próximas tivessem seu acesso liberado, bem como o restante do mundo, como vemos nos dias de hoje (SANTANA, 2006).

Twitter: *Micro blog* criado em março de 2006 por Jack Dorsey, Evan Williams e Biz Stone como um projeto paralelo da *Odeo* (empresa de *podcasting*). A ideia surgiu de Dorsey durante uma reunião de discussão de ideias (*brainstorming*) em que falava sobre um serviço de trocas de *status*, como um SMS. A explosão do *Twitter* aconteceu no mesmo ano em um festival de música e filmes para novos talentos, que trouxe a tecnologia como foco através de conferências interativas. O festival atraiu muitos criadores e empresários do ramo tecnológico para mostrar suas ideias (OLIVEIRA, 20015; SMAAL, 2010).

WhatsApp: A história do aplicativo começa quando seu criador Jan Koum, fundador e CEO do WhatsApp, nascido em Kiev na Ucrânia, tornou-se imigrante nos Estados Unidos ainda na infância e viveu pobreza em grande parte da sua vida. Em 2009 surgiu a ideia de criar o aplicativo que daria uma reviravolta na sua vida. O aplicativo inicialmente foi disponibilizado apenas para *Iphone* e posteriormente devido ao grande sucesso para o *Android*. O sucesso do aplicativo é tão grande que hoje a plataforma já conta com mais de 1 Bilhão de usuários e continuam crescendo mês a mês (KLEIMA, 2018).

Instagram: Aplicativo inicialmente criado para fazer *check-in* em fotografia. Foi criado pelo brasileiro Mike Krieger e seu amigo norte americano Kevin Systrom, inicialmente o aplicativo chamava-se *Burbn*, porém era muito complicado de usar e resolveram

simplificar, e em 2010 foi que surgiu com o nome que conhecemos hoje (*Instagram*) foi lançado originalmente para o sistema IOS e posteriormente devido ao grande sucesso, foi lançado para outras plataformas (KINAST, 2020).

4. Experimento

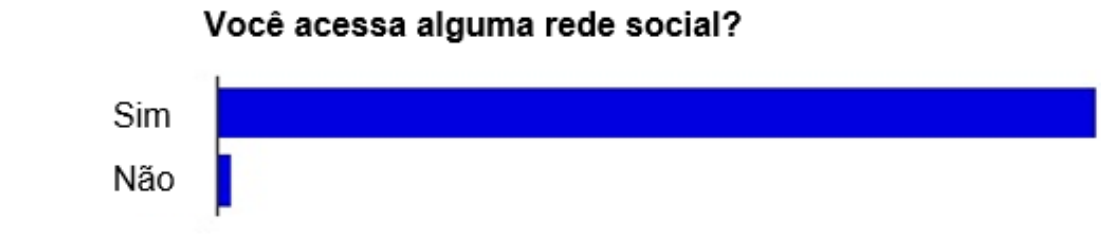
A pesquisa (figura 1) foi aplicada de forma, qualitativa e quantitativa, utilizando técnica de coleta e análise de dados interativos. Trata-se de uma pesquisa baseada em questões do uso diário, dificuldades e qual grau de importância dada ao quesito segurança de dados. O objetivo do estudo de caso é de criar um perfil de usuário mais consciente com relação às necessidades em privar seus dados de pessoas mal intencionadas. A pesquisa levou em conta a forma de conexão, modo de acesso e quanto à necessidade da segurança de seus dados nas redes sociais.

Figura 1: pesquisa
Fonte: Própria

4.1 Pesquisa

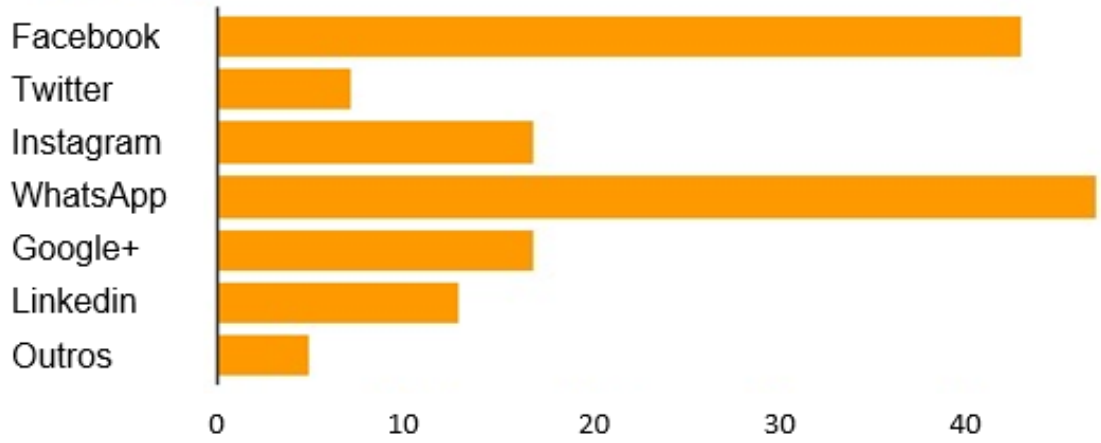
A pesquisa estimulada (figura 2) levou em conta a forma de conexão (figura 3), modo utilizado para o acesso, qual o local e sistema operacional (figura 4) e quanto à preocupação dada ao quesito segurança de seus dados nas redes sociais (figura 3). A

coleta dos dados foi efetuada de forma aleatória e de diferentes faixas etárias, ficando disponível no mês Maio, hospedada na ferramenta *Google Form*.



Sim	**50**	**98%**
Não	**1**	**2%**

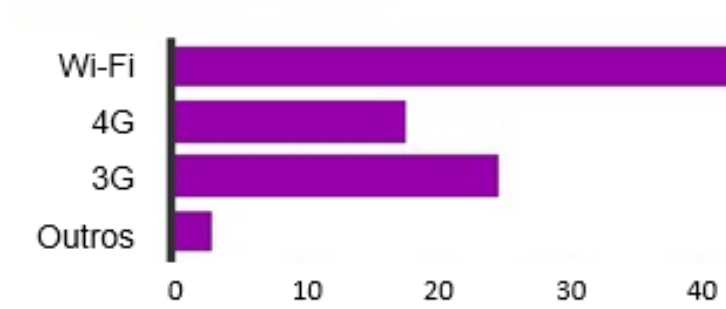
Qual?



Facebook	43	84.3%
Twitter	7	13.7%
Instagram	17	33.3%
WhatsApp	47	92.2%
Google+	17	33.3%
Linkedin	13	25.5%
Outros	5	9.6%

Figura 2: pesquisa estimulada
Fonte: Própria

Qual a Forma de Conexão?



Wi-Fi	49	96.1%
4G	18	35.3%
3G	25	49%
Outros	3	5.9%

Utiliza Antivírus?

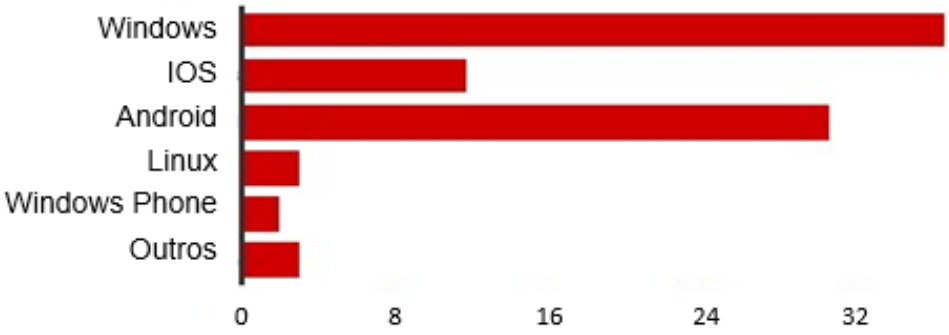
Sim	34	66.7%
Não	13	25.5%
Não sabe	4	7.8%

Relacionado a Roubo de Dados na Internet. Qual sua Preocupação Sobre o Assunto?

Muita	35	68.6%
Pouca	15	29.4%
Nenhuma	1	2%

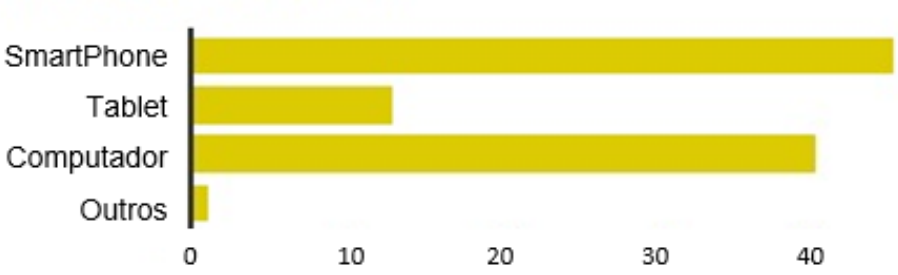
Figura 3: formas de conexão
Fonte: Própria

Qual é o Sistema Operacional Usado?



Windows	37	72.5%
IOS	12	23.5%
Android	31	60.8%
Linux	3	5.9%
Windows Phone	2	3.9%
Outros	3	5.9%

Qual a Forma de Acesso?



SmartPhone	45	88.2%
Tablet	13	25.5%
Computador	40	78.4%
Outros	1	2%

Qual o Local Usado para o Acesso?

Casa	51	100%
Trabalho	31	60.8%
Outros	12	23.5%

Figura 4: pesquisa sistema operacional
Fonte: Própria

4.2 Discussão dos Resultados

A figura 2, nos mostra que do total de usuários que responderam à pesquisa sendo um total de 51 pessoas, 98% acessam algum tipo de rede social e apenas 1% não faz usa da mesma. Observamos ainda que entre as mais acessadas o WhatsApp lidera com 92.2% seguida da Facebook com 84.3% de usuários que as acessam. Sendo que a classificação do tipo de rede social utilizada pelos entrevistados se deu por prioridade dos usuários, ou seja, cada usuário entrevistado pode acessar mais de uma rede social de acordo com sua necessidade ou preferência.

Com relação ao tipo de conexão e ao uso de proteção como antivírus podemos ver na figura 3, 96.1% utiliza na maior parte do tempo Wi-Fi seguido de 3G com 49%, os tipos de acesso. Apresenta-se na figura 3 os mais comuns, sendo que o Wi-Fi é muito utilizado quando o usuário se encontra em casa ou no trabalho, estando na rua o usuário utiliza na maioria das vezes o 3G ou 4G disponível em seu dispositivo móvel como SmartPhone (88.2%) ou Tablet (25.5%) por exemplo como podemos observar na figura 4. Com relação a utilização de antivírus 66.7% (figura 3) dos usuários utiliza algum tipo sendo que temos diversos disponível de forma free ou pago, 25.5% não utiliza nenhuma proteção e 7.8% não sabem se usam ou não quiseram responder.

Nota-se ainda na figura 3 que na sua grande maioria 68.6%, os usuários tem grande preocupação relacionados a roubo de dados via internet. Sabe-se que é possível se fazer roubos de arquivos, senhas e dados pessoais mesmos estes estando em seu dispositivo móvel desde que este tenha acesso a internet, mesmo o dono não fazendo uso de redes sociais, fazendo uma simples busca em algum site. Sendo que 29.4% tem pouca preocupação e apenas 1% não se preocupa com roubos via internet.

Com relação ao sistema operacional utilizado nota-se na figura 4 que o mais utilizado é o Windows com 72.5%, seguido do Android 60.8% e o IOS 23.5%, lembrando que o usuário pode utilizar mais de um sistema operacional. Pois os mesmos podem acessar as redes sociais de vários dispositivos, sendo computador com 78.4%, SmartPhone com 88.2% e tablet com 25.5% (figura 4). Os usuários utilizam as redes sociais na sua maioria (100%) em casa, porém hoje muitas das empresas utilizam o WhatsApp como meio de comunicação rápida entre seus colaboradores. Mas destaca-se

que um número relativamente alto de 60.8% utilizando redes sociais no local de trabalho, sendo que podem estar utilizando de outras redes sociais e não apenas o WhatsApp e vale lembrar que exclusivamente para trabalho.

5. Mecanismos de Segurança

Existe diversos meios de evitar ou até mesmo mitigar determinadas invasões ou acessos indevidos aos dados, seja armazenado in loco ou nas nuvens, para isso podemos aplicar mecanismos de forma física ou lógica.

- Os controles físicos podem ser definidos como barreiras de limitam o acesso direto a informação por meio de infraestrutura, mantendo a integridade dos dados através de um *hardware* controlado por *software.* Exemplo para esse caso é o uso do servidor de acesso, onde existem políticas que são controladas por um sistema operacional, mas necessitam do *hardware*.
- O controle lógico diferentemente do meio físico não depende de um *hardware* especifico para tal controle, sendo dessa forma controlado eletronicamente por um determinado *software*, previamente instalado na estação em uso. Os controles lógicos são apoiados por mecanismos de segurança, tais como: Criptografia e assinatura digital, porém corriqueiramente é encontrado no ambiente web em forma que avaliadores de senhas (ZANIQUELLI, 2009).

6. Principais Riscos

Compartilhar informações com amigos, colegas ou parentes, através de um site ou aplicativo é a forma mais rápida disponível no momento, se compararmos com os tempos onde a comunicação era feita somente através de correspondência (Carta ou telefone), porém é necessário que se tenha clareza dos riscos proporcionados por essa evolução tecnológica.

De acordo com estudos anteriores, muitos usuários não utilizam as configurações de privacidade, deixando dessa forma suas informações vulneráveis a criminosos ou, até mesmo outros riscos pertencentes à rede.

Segundo estudos levantados pela empresa Sophos, que é especializada em segurança da informação, o número de ataques virtuais vem crescendo ano a ano nas redes mais utilizadas, que são Facebook e Twitter. Nesse estudo 57% dos usuários já foram vítimas de spam e 36% já receberam malware através de uma das redes sociais. Isso indica um aumento de 70% referente aos anos anteriores (CERT. br, 2006).

Conforme levantamento efetuado pela empresa Stratecast 22% dos usuários de redes sociais já caíram em alguma armadilha virtual. A atenção nesse caso deve ser redobrada, pois mesmo postagens de pessoas conhecidas oferecem riscos. Para exemplo, podemos pensar em casos bastante comuns: Quando os usuários veem algo publicado por alguém que está em sua lista de amigos, clicam sem pensar duas vezes, e é aí que mora o perigo, pode ser uma cilada virtual (CERT. br, 2006).

As principais formar de ataques na rede social ocorre basicamente de 5 maneiras (CERT. br, 2006):

- Oferta imperdível, essa forma de ataque consiste em ofertas convidativas, na maioria das vezes oferecendo emprego com altos ganhos em pouco tempo, onde na maioria das vezes um programa malicioso invade contas de pessoas reais e sai espalhando a tal falsa promessa. De quebra, ainda marca vários amigos na mesma publicação.
- Testes como: “Descubra que personagem da novela você é?” ou “Calcule a sua idade real” podem ser apenas um disfarce para um programa malicioso. Se for participar de um jogo deste tipo, fique atento para as permissões exigidas. Jamais aceite liberar informações pessoais ou dos seus amigos e verifique antes de entrar na brincadeira, se a empresa que produziu o aplicativo é confiável.
- Notícias falsas geralmente se aproveitam da curiosidade do usuário para fazer o ataque, direcionando para link externo, no site para qual o usuário é direcionado, ao clicar na notícia, pode trazer arquivos contaminados para serem baixados. E no momento da curiosidade, o internauta baixa qualquer coisa.
- Curtida perigosa, os botões de compartilhamento de redes sociais estão presentes em milhares de sites. Com a ajuda deles, fica bem mais simples compartilhar links e notícias com amigos. Por esta razão, criminosos virtuais criam páginas falsas, com

botões igualmente fajutos. Ao clicar neles o usuário baixa um programa e contamina o computador.

- Extensões maliciosas, assim como smartphones contam com aplicativos para facilitar a navegação, alguns *browsers*, como o *Chrome* e o *Firefox*, também permitem extensões para aperfeiçoar a experiência dos usuários nas redes sociais.

Mas existem versões destes aplicativos que são malwares disfarçados. Por isso a orientação é que baixe somente um complemento de loja oficial, e verifique antes as avaliações dos usuários que já experimentaram aquele programa (CERT. br, 2006, p.08).

7. Privacidade e Segurança

Ficou evidenciado anteriormente que, existem diversas formas de ataques a redes, seja com a finalidade de denigrir a imagem ou até mesmo furto de informações, mas assim como existem diversas formas de invasão, existem também as formas de prevenção. A seguir iremos citar algumas (ALECRIM, 2006):

- Efetue logout, ao acessar seu perfil em uma rede social, seja qual for o serviço pede que sua senha fique cadastrada para um próximo acesso, até mesmo para facilitar seu acesso, mas isso implica também em um grande risco para o usuário, pois tal procedimento pode facilitar a invasão o dispositivo de casso seja compartilhado com mais pessoas.
- Senhas, especialistas indicam que os usuários não utilizem senhas fracas, tais como; nome de parentes, data de aniversário, placa de carro, etc. sempre de preferência para as senhas que misturam letras, números e até mesmo símbolos especiais. Recomenda-se utilizar senhas acima de 6 caracteres e que as mesmas não sejam guardadas em dispositivos de fácil acesso se for o caso anote-a em um local de difícil acesso, até que a mesma seja decorada e após isso a destrua.
- Navegadores dê preferência a navegadores mais utilizados, pois esses são os que recebem maiores número de atualizações, a fim de manter um nível de segurança alto, geralmente utilizam HTML5.
- Antivírus, muitos usuários ainda não dão a devida atenção para a necessidade da instalação de um *software* que mantenha o ambiente seguro, porém nos dias atuais é um

software indispensável. Além de manter a segurança para o mundo externo é necessário que o mesmo esteja sempre com suas definições atualizadas, pois dessa forma poderá agir contra os diversos vírus que são criados todos os dias.

- Informações pessoais, não revelar informações pessoais, onde desconhecidos poderão ter o acesso irrestritamente, evite dar detalhes da escola ou faculdade em qual estuda, do lugar onde trabalha e principalmente onde reside. Evite disponibilizar dados detalhados sobre sua pessoa, como viagens, passeios, e jamais divulgue sua geolocalização.

8. Marco Civil

O Marco Civil é a lei que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para a União, dos Estados, do Distrito Federal e dos Municípios.

Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, dados pessoais ou comunicações por provedores de conexão e de aplicações de internet no território nacional, deverão ser obrigatoriamente respeitados à legislação brasileira, o direito à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas.

> Com o intuito de assegurar a liberdade de expressão de impedir a censura, o provedor de aplicações da internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado terceiros se, após ordem judicial especifica, não tomar as providencias para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (Congresso Nacional, 2014, p. 6).

Guarda de logs: obriga os provedores de acesso a guardarem os registros de conexão dos usuários pelo período de um ano, sob sigilo total. Nesses registros deverá constar apenas o IP do usuário, datas e hora inicial e final da conexão (ATHENIENSE, 2012).

Retirada de conteúdo: delimita a quem se deve recorrer para pedir a remoção de conteúdo que seja ofensivo ou danoso a um terceiro. O conteúdo só poderá ser retirado do ar após a ordem judicial, que deverá ser motivada contra o usuário que postou o

conteúdo e não contra o provedor de acesso. Isso impediria a censura na internet, como quando o *Youtube* foi retirado do ar no Brasil devido a um vídeo postado por um de seus usuários.

CONSIDERAÇÕES FINAIS

As redes sociais promovem a interação com pessoas de diferentes localidades e nacionalidades, possuem suas políticas de uso e privacidade, a fim de criar normas para garantir a segurança de seus usuários ou até mesmo a punição daqueles que descumprem os termos de usabilidade.

Devido sua ampla inclusão nas diversas camadas sociais, fica evidenciado pelo grande número de reportagens em jornais, revistas e blogs, o crescente número de ataques virtuais e em sua maioria aplicado a rede social, seja por falta de conhecimento ou por excesso de confiança de quem a utiliza.

Os diversos aspectos relacionados à segurança precisam e deverão ser considerados pelos usuários, como a utilização de senhas baseadas em criptografias mais fortes, utilização de dispositivos de segurança, tais como: Antivírus e as demais configurações necessárias para uma navegação íntegra e segura.

A regulamentação do Marco Civil foi um passo importante para que os dados, deveres e crimes cometidos no ambiente virtual, sofressem suas penalidades cabidas em lei. A legislação brasileira deve prevalecer sobre as leis internacionais citadas nos contratos, desde que a coleta desses dados seja efetuada no Brasil, com essa medida é possível garantir a neutralidade da rede e permitir que o usuário seja indenizado em caso de violação de seus dados.

Por fim, sabemos que devido ao dinamismo do meio virtual, podemos dizer que o número de ataques é crescente, necessitando dessa forma, mais segurança dos dados, e responsabilidade das informações que são disponibilizadas. De acordo, esse artigo poderá servir para futuras pesquisas e acima disso, que sirva de norte para a conscientização de usuários de redes sociais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALECRIM, Emerson. “Dicas de Segurança na Internet.” 2006. Disponível em: <http://www.infowester.com/dicaseguranca.php>. Acesso em: 08 maio 2016.

ATHENIENSE, Alexandre. “Perguntas e Respostas Sobre Marco Civil da Internet.” 2012. Disponível em: <http://alexandre-atheniense.jusbrasil.com.br/noticias/2819686/perguntas-e-respostas-sobre-marco-civil-da-internet>. Acesso em: 07 maio 2016.

BENETTI, Ticianoi. “Pilares da Segurança da informação.” 2015. Disponível em: <www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid>. Acesso em: 30 abril 2016.

CERT.br. “Cartilha de Segurança para Internet.” 2006. Disponível em <http://cartilha.cert.br/seguranca/>. Acesso em: 06 maio 2016.

CONGRESSO NACIONAL. “PROJETO DE LEI DO SENADO Nº 180, DE 2014”. 2014. Disponível em: <https://www.congressonacional.leg.br/>. Acesso em: 05 maio 2016.

DAQUINO, Fernando. “História Das Redes Sociais.” 2012. Disponível em: <http://www.tecmundo.com.br/redes-sociais/33036-a-historia-das-redes-sociais-como-tudo-comecou.htm>. Acesso em: 03 maio 2016.

KINAST, Priscila. “A história do Instagram.” 2020. Disponível em: <https://www.oficinadanet.com.br/historiasdigitais/29859-historia-do-instagram>. Acesso em: 27 abril 2020.

KLEIMA, Nilton. “A história do WhatsApp, o rei dos mensageiros.” 2018. Disponível em: <https://www.tecmundo.com.br/dispositivos-moveis/125894-historia-whatsapp-rei-mensageiros-video.htm>. Acesso em: 27 abril 2020.

OLIVEIRA, Felipe. “História do Twitter”. 2015. Disponível em: <https://www.meucupom.com/blog/conheca-historia-do-whatsapp>. Acesso em: 03 maio 2016.

SANTANA, Ana. “História do Facebook.” 2006. Disponível em: <http://www.infoescola.com/internet/historia-do-facebook>. Acesso em: 04 maio 2016.

SMAAL, Beatriz. “História do Twitter.” 2010. Disponível em: <http://www.tecmundo.com.br/rede-social/3667-a-historia-do-twitter.htm>. Acesso em: 27 abril 2016.

WENDT, Emerson. “Wendt.” 2016. Disponível em: <http://www.emersonwendt.com.br>. Acesso em: 28 abril 2016.

ZANIQUELLI, Tiago. “Convergência Segurança Física e Lógica.” 2009. Disponível em: <http://www.devmedia.com.br/convergencia-seguranca-fisica-e-logica/15760>. Acesso em: 03 maio 2016.